

## WEST Search History

[Hide Items](#)
[Restore](#)
[Clear](#)
[Cancel](#)

DATE: Tuesday, June 20, 2006

Hide?	Set Name	Query	Hit Count
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L43	726/2,5,8,9,10,20.ccls. and (biometric and (knowledge or password) and decrypt\$7 and compar\$7 and (generat\$6 near4 key))	33
<input type="checkbox"/>	L42	L41 and (encrypt\$7 near4 identify\$7)	18
<input type="checkbox"/>	L41	(biometric and (knowledge or password) and decrypt\$7 and compar\$7 and (generat\$6 near4 key) and (bind\$6 or bound))and token	263
<input type="checkbox"/>	L40	(biometric and (knowledge or password) and decrypt\$7 and compar\$7 and (generat\$6 near4 key) and (bind\$6 or bound))	635
<input type="checkbox"/>	L39	(biometric and (knowledge or password) and decrypt\$7 and compar\$7 and (generat\$6 near4 key) and (bind\$6 or bound)).clm.	2
<input type="checkbox"/>	L38	L37 and (encrypt\$7 near2 biometric)	20
<input type="checkbox"/>	L37	713/182.ccls.	936
<input type="checkbox"/>	L36	L35 and challenge and salt	4
<input type="checkbox"/>	L35	L34 and (unlock\$7 or decrypt\$6)	130
<input type="checkbox"/>	L34	L33 and (private adj key)	151
<input type="checkbox"/>	L33	(380/\$.ccls. or 713/\$.ccls. or 705?\$.ccls. or 726/\$.ccls. or 709/\$.ccls.) and ((multi\$6 near3 factor\$7) and authentication)	389
<input type="checkbox"/>	L32	L29 and (unlock\$7 or decrypt\$7)and challenge\$2 and salt	3
<input type="checkbox"/>	L31	L29 and (unlock\$7 or decrypt\$7)and challenge\$2	69
<input type="checkbox"/>	L30	L29 and (unlock\$7 or decrypt\$7)	106
<input type="checkbox"/>	L29	L28 and (private adj key)	125
<input type="checkbox"/>	L28	(380/\$.ccls. or 714/\$.ccls. or 705?\$.ccls. or 726/\$.ccls. or 709/\$.ccls.) and ((multi\$6 near3 factor\$7) and authentication)	329
		<i>DB=PGPB; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L27	((token and random adj value and salt and token adj id and password and key and challenge))	1
		<i>DB=PGPB,USPT,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L26	((token and random adj value and salt and token adj id and password and key and challenge))	1
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L25	705/\$.ccls. and ((token and random adj value and salt and token adj id and password and key and challenge))	0
<input type="checkbox"/>	L24	726/\$.ccls. and ((token and random adj value and salt and token adj id and password and key and challenge))	0
<input type="checkbox"/>	L23	713/\$.ccls. and ((token and random adj value and salt and token adj id and password and key and challenge))	1

<input type="checkbox"/>	L22	709/\$.ccls. and ((token and random adj value and salt and token adj id and password and key and challenge))	0
<input type="checkbox"/>	L21	(token and random adj value and salt and token adj id and password and key and challenge).clm.	1
<input type="checkbox"/>	L20	(token and random adj value and salt and token adj id and password and key and challenge).clm.	0
<i>DB=PGPB,USPT,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>			
<input type="checkbox"/>	L19	L18 and (multi\$3 near3 factor\$2)	4
<input type="checkbox"/>	L18	L17 and (PIN and smart adj card)	51
<input type="checkbox"/>	L17	(705/67).ccls. and biometric	102
<input type="checkbox"/>	L16	705/67. and (biometric or fingerprint)	0
<input type="checkbox"/>	L15	L14 and factor\$6	12
<input type="checkbox"/>	L14	((Scheidt near2 Edward) or (Domangue near2 Ersin)) and authentication and biometric	15
<input type="checkbox"/>	L13	((Scheidt near2 Edward) or (Domangue near2 Ersin)) and authentication	19
<input type="checkbox"/>	L12	L11 and (multi\$3 near2 factor\$2)	3
<input type="checkbox"/>	L11	L10 and (encrypt\$7 same (generat\$6 near2 key))	38
<input type="checkbox"/>	L10	L9 and (password and (smart adj card or token))	164
<input type="checkbox"/>	L9	(713/168  713/176).ccls. and (biometric)	316
<input type="checkbox"/>	L8	(713/166  713/183  713/184  713/185  713/186).ccls. and (biometric and authenticat\$7 and multi adj factor)	7
<i>DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>			
<input type="checkbox"/>	L7	(6,317,834 and token)	2
<input type="checkbox"/>	L6	((713/184  713/185  713/186)!.CCLS.))	1309
<input type="checkbox"/>	L5	((713/184  713/185  713/186)!.CCLS.))	1309
<input type="checkbox"/>	L4	(6,317,834 and token)	2
<input type="checkbox"/>	L3	((713/184  713/185  713/186)!.CCLS.))	1309
<input type="checkbox"/>	L2	((713/184  713/185  713/186)!.CCLS.))	1309
<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>			
<input type="checkbox"/>	L1	6,845,453.pn.	2

END OF SEARCH HISTORY


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

token +"multiple" +" factors" +authentication + encryption+bi

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used token multiple  
factors authentication encryption biometric password

Found 512 of 178,880

 Sort results  
by


[Save results to a Binder](#)
[Try an Advanced Search](#)
[Try this search in The ACM Guide](#)

 Display  
results


[Search Tips](#)
☐ Open results in a new  
window

Results 1 - 20 of 200

 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

 Relevance scale ☐ ☐ ☐ ☐ ☐

### 1 [Strong password-only authenticated key exchange](#)



David P. Jablon

 October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Publisher: ACM Press

 Full text available: [pdf\(1.52 MB\)](#)

 Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

### 2 [Paranoid penguin: two-factor authentication](#)



Corey Steele

 November 2005 **Linux Journal**, Volume 2005 Issue 139

Publisher: Specialized Systems Consultants, Inc.

 Full text available: [html\(17.28 KB\)](#)

 Additional Information: [full citation](#), [abstract](#), [index terms](#)

?

### 3 [Unified login with pluggable authentication modules \(PAM\)](#)



Vipin Samar

 January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

 Full text available: [pdf\(1.12 MB\)](#)

 Additional Information: [full citation](#), [references](#), [index terms](#)

### 4 [Integrating security in a large distributed system](#)



M. Satyanarayanan

 August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3

Publisher: ACM Press

 Full text available: [pdf\(2.90 MB\)](#)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

[terms](#), [review](#)

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

##### 5 [Protecting applications with transient authentication](#)



Mark D. Corner, Brian D. Noble

May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**

**Publisher:** ACM Press

Full text available: [pdf\(294.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

##### 6 [Unlinkable serial transactions: protocols and applications](#)



Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag

November 1999 **ACM Transactions on Information and System Security (TISSEC)**,  
Volume 2 Issue 4

**Publisher:** ACM Press

Full text available: [pdf\(184.87 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

**Keywords:** anonymity, blinding, cryptographic protocols, unlinkable serial transactions

##### 7 [Authentication and authorization: Securing passwords against dictionary attacks](#)



Benny Pinkas, Tomas Sander

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

**Publisher:** ACM Press

Full text available: [pdf\(216.72 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user' ...

##### 8 [Evaluating interaction: research papers: Design and evaluation of a shoulder-surfing resistant graphical password scheme](#)




-  Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean-Camille Birget  
May 2006 **Proceedings of the working conference on Advanced visual interfaces AVI '06**

**Publisher:** ACM Press

Full text available:  [pdf\(523.36 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shoulder-surfing and is a known risk, of special concern when authenticating in public places. Until recently, the only defense against shoulder-surfing has been vigilance on the part of the user. This paper reports on the design and evaluation of a gam ...

**Keywords:** authentication, convex hull click scheme, graphical passwords, password security, shoulder-surfing, usable security

- 9 Security and usability: the case of the user authentication methods 

-  Christina Braz, Jean-Marc Robert  
April 2006 **Proceedings of the 18th international conference on Association Francophone d'Interaction Homme-Machine IHM '06**


**Publisher:** ACM Press

Full text available:  [pdf\(292.60 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


The usability of security systems has become a major issue in research on the efficiency and user acceptance of security systems. The authentication process is essential for controlling the access to various resources and facilities. The design of usable yet secure user authentication methods raises crucial questions concerning how to solve conflicts between security and usability goals.

**Keywords:** access control, human factors, security usability, user authentication, user interface design

- 10 Security: Zero-interaction authentication 

-  Mark D. Corner, Brian D. Noble  
September 2002 **Proceedings of the 8th annual international conference on Mobile computing and networking**


**Publisher:** ACM Press

Full text available:  [pdf\(273.30 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryptographic file system does not fully address this problem. Such systems ask the user to imbue them with long-term authority for decryption, but that authority can be used by anyone who physically possesses the machine. Forcing the user to frequently reestablish his identity is intrusive, encouraging him to disable encryption. Our solution to this problem is Zero- ...

**Keywords:** cryptographic file systems, mobile computing, stackable file systems, transient authentication

- 11 Password hardening based on keystroke dynamics 

-  Fabian Monrose, Michael K. Reiter, Susanne Wetzel  
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

**Publisher:** ACM Press

Full text available:  pdf(1.01 MB)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present a novel approach to improving the security of passwords. In our approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both online and offline attackers. In addition, our scheme automatically adapts to gradual changes in a user's typing patterns while maintaining the s ...

12 [General storage protection techniques: Securing distributed storage: challenges, techniques, and systems](#)



Vishal Kher, Yongdae Kim

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available:  pdf(294.61 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

**Keywords:** authorization, confidentiality, integrity, intrusion detection, privacy


13 [Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks](#)



Haidong Xia, José Carlos Brustoloni

May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**

Publisher: ACM Press

Full text available:  pdf(770.11 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

**Keywords:** HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

14 [DIM frameworks: Federated identity management for protecting users from ID theft](#)



Paul Madsen, Yuzo Koga, Kenji Takahashi

November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM '05**

Publisher: ACM Press

Full text available:  pdf(143.83 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Federated identity management is sometimes criticized as exacerbating the problem of online identity theft, based as it is on the idea of connecting together previously separate

islands of identity information. This paper explores this conjecture, and argues that, while such linkages do undeniably increase the potential scope of a successful theft of identity information, this risk is more than offset by the much greater value federated identity, in combination with strong authentication, offers ...

**Keywords:** federated identity, identity theft, phishing

## 15 Implementing protocols via declarative event patterns



Robert J. Walker, Kevin Viggers

October 2004 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 12th ACM SIGSOFT twelfth international symposium on Foundations of software engineering SIGSOFT '04/FSE-12**, Volume 29 Issue 6

**Publisher:** ACM Press

Full text available: [pdf\(145.61 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper introduces declarative event patterns (DEPs) as a means to implement protocols while improving their traceability, comprehensibility, and maintainability. DEPs are descriptions of sequences of events in the execution of a system that include the ability to recognize properly nested event structures. DEPs allow a developer to describe a protocol at a high-level, without the need to express extraneous details. A developer can indicate that specific actions be taken when a given patte ...

**Keywords:** aspect-oriented programming, comprehensibility/maintainability, context-free grammars, context-sensitive join points, event patterns, instrumentation, parsing, traceability

## 16 The battle against phishing: Dynamic Security Skins



Rachna Dhamija, J. D. Tygar

July 2005 **Proceedings of the 2005 symposium on Usable privacy and security SOUPS '05**

**Publisher:** ACM Press

Full text available: [pdf\(398.10 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Phishing is a model problem for illustrating usability concerns of privacy and security because both system designers and attackers battle using user interfaces to guide (or misguide) users. We propose a new scheme, Dynamic Security Skins, that allows a remote web server to prove its identity in a way that is easy for a human user to verify and hard for an attacker to spoof. We describe the design of an extension to the Mozilla Firefox browser that implements this scheme. We present two novel inte ...

## 17 Puzzles and users: A PIN-entry method resilient against shoulder surfing



Volker Roth, Kai Richter, Rene Freidinger

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**

**Publisher:** ACM Press

Full text available: [pdf\(301.35 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Magnetic stripe cards are in common use for electronic payments and cash withdrawal. Reported incidents document that criminals easily pickpocket cards or skim them by swiping them through additional card readers. Personal identification numbers (PINs) are obtained by shoulder surfing, through the use of mirrors or concealed miniature cameras. Both elements, the PIN and the card, are generally sufficient to give the criminal full access to the victim's account. In this paper, we present alter ...

**Keywords:** ATM, PIN, cognitive trapdoor games, password, shoulder surfing

18 Applications: YouServ: a web-hosting and content sharing tool for the masses



Roberto J. Bayardo Jr., Rakesh Agrawal, Daniel Gruhl, Amit Somani

May 2002 **Proceedings of the 11th international conference on World Wide Web**

**Publisher:** ACM Press

Full text available: pdf(238.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

YouServ is a system that allows its users to pool existing desktop computing resources for *high availability* web hosting and file sharing. By exploiting standard web and internet protocols (e.g. HTTP and DNS), YouServ does not require those who access YouServ-published content to install special purpose software. Because it requires minimal server-side resources and administration, YouServ can be provided at a very low cost. We describe the design, implementation, and a successful intrane ...

**Keywords:** decentralized systems, p2p, peer-to-peer networks, web hosting

19 Intrusion detection and modeling: Augmenting storage with an intrusion response



primitive to ensure the security of critical data

Ashish Gehani, Surendar Chandra, Gershon Kedem

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

**Publisher:** ACM Press

Full text available: pdf(326.59 KB) Additional Information: [full citation](#), [abstract](#), [references](#)

Hosts connected to the Internet continue to suffer attacks with high frequency. The use of an intrusion detector allows potential threats to be flagged. When an alarm is raised, preventive action can be taken. A primary goal of such action is to assure the security of the data stored in the system. If this operation is effected manually, the delay between the alarm and the response may be enough for an intruder to cause significant damage. The alternative proposed in this paper is to provide a re ...

20 Fine-grained control of security capabilities



Dan Boneh, Xuhua Ding, Gene Tsudik

February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1

**Publisher:** ACM Press

Full text available: pdf(128.09 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

**Keywords:** Certificate Revocation, Digital Signatures, Public Key Infrastructure

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)